НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20230130.12 | 30 января 2023 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в ОС Junos серии SRX 5000

Идентификатор уязвимости	MITRE: CVE-2023-22408
Идентификатор программной ошибки	CWE-129: Некорректная проверка индекса массива
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевого устройства посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной обработкой запросов.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	ОС Junos серия SRX 5000: версии с 20.4 до 20.4R3-S5; версии с 21.1 до 21.1R3-S4; версии с 21.2 до 21.2R3-S3; версии с 21.3 до 21.3R3-S3; версии с 21.4 до 21.4R3-S2; версии с 22.1 до 22.1R2-S2, 22.1R3; версии с 22.2 до 22.2R3; версии с 22.3 до 22.3R1-S1, 22.3R2.
Рекомендации по устранению	Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.
Дата выявления	12 января 2023 г.
Дата обновления	24 января 2023 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Вектор атаки (AV)	Сетевой (N)

Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Отсутствует (N)
Влияние на целостность (I)	Отсутствует (N)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Не определено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Не определено
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2023-22408 https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-SRX-5000-Series-Upon-processing-of-a-specific-SIP-packet-an-FPC-can-crash-CVE-2023-22408?language=en_US